

EXHIBIT 1

Person Filing: Keith Beauchamp

Address (if not protected): 2800 North Central Avenue, Suite 1900

City, State, Zip Code: Phoenix, AZ 85004

Telephone: (602)381-5490

Email Address: kbeauchamp@cblawyers.com

Representing ☐ Self or ☒ Attorney for:

Lawyer's Bar Number: 012434, Issuing State: AZ

Clerk of the Superior Court
*** Electronically Filed ***
A. Marquez, Deputy
1/13/2025 1:42:37 PM
Filing ID 19154842**SUPERIOR COURT OF ARIZONA
IN MARICOPA COUNTY**Case Number: **CV2025-001530**BLUE CROSS AND BLUE SHIELD OF ARIZONA, INC, et al.

Name of Plaintiff

SUMMONS

AND

CHANGE HEALTHCARE PRACTICE MANAGEMENT SOLUTION
INC., et al.

Name of Defendant

WARNING: This is an official document from the court that affects your rights. Read this carefully.
If you do not understand it, contact a lawyer for help.**FROM THE STATE OF ARIZONA TO: CHANGE HEALTHCARE PAYER PAYMENT INTEGRITY, LL**

Name of Defendant

1. **A lawsuit has been filed against you.** A copy of the lawsuit and other court papers are served on you with this "Summons".
2. If you do not want a judgment or order taken against you without your input, you must file an "Answer" or a "Response" in writing with the court and pay the filing fee. If you do not file an "Answer" or "Response" the other party may be given the relief requested in his/her Petition or Complaint. To file your "Answer" or "Response" take, or send, the "Answer" or "Response" to Clerk of the Superior Court, or electronically file your Answer through one of Arizona's approved electronic filing systems at <http://www.azcourts.gov/efilinginformation>. Mail a copy of your "Response" or "Answer" to the other party at the address listed on the top of this Summons. Note: If you do not file electronically you will not have electronic access to the document in this case.

3. If this “Summons” and the other court papers were served on you by a registered process server or the Sheriff, within the State of Arizona, your “Response” or “Answer” must be filed within TWENTY (20) CALENDAR DAYS from the date you were served, not counting the day you were served. If this “Summons” and the other papers were served on you by a registered process server or the Sheriff outside the State of Arizona, your Response must be filed within THIRTY (30) CALENDAR DAYS from the date you were served, not counting the day you were served. Service by a registered process server or the Sheriff is complete when made. Service by Publication is complete thirty (30) days after the date of the first publication.
4. You can get a copy of the court papers filed in this case from the Petitioner at the address at the top of this paper, or from the Clerk of the Superior Court.
5. Requests for reasonable accommodation for persons with disabilities must be made to the office of the judge or commissioner assigned to the case, at least ten (10) judicial days before your scheduled court date.
6. Requests for an interpreter for persons with limited English proficiency must be made to the office of the judge or commissioner assigned to the case at least ten (10) judicial days in advance of your scheduled court date.

SIGNED AND SEALED this Date: *January 13, 2025*

JEFF FINE
Clerk of Superior Court

By: *A. MARQUEZ*
Deputy Clerk



If you would like legal advice from a lawyer, contact Lawyer Referral Service at 602-257-4434 or <https://maricopabar.org>. Sponsored by the Maricopa County Bar Association.

Person Filing: Keith Beauchamp

Address (if not protected): 2800 North Central Avenue, Suite 1900

City, State, Zip Code: Phoenix, AZ 85004

Telephone: (602)381-5490

Email Address: kbeauchamp@cblawyers.com

Representing ☐ Self or ☒ Attorney for:

Lawyer's Bar Number: 012434, Issuing State: AZ

Clerk of the Superior Court
*** Electronically Filed ***
A. Marquez, Deputy
1/13/2025 1:42:37 PM
Filing ID 19154839SUPERIOR COURT OF ARIZONA
IN MARICOPA COUNTY

Case Number: CV2025-001530

BLUE CROSS AND BLUE SHIELD OF ARIZONA, INC, et al.

Name of Plaintiff

SUMMONS

AND

CHANGE HEALTHCARE PRACTICE MANAGEMENT SOLUTION
INC., et al.

Name of Defendant

WARNING: This is an official document from the court that affects your rights. Read this carefully.
If you do not understand it, contact a lawyer for help.CHANGE HEALTHCARE PRACTICE MANAGEMENT SOLU
FROM THE STATE OF ARIZONA TO: INC. _____

Name of Defendant

- 1. A lawsuit has been filed against you.** A copy of the lawsuit and other court papers are served on you with this "Summons".
- If you do not want a judgment or order taken against you without your input, you must file an "Answer" or a "Response" in writing with the court and pay the filing fee. If you do not file an "Answer" or "Response" the other party may be given the relief requested in his/her Petition or Complaint. To file your "Answer" or "Response" take, or send, the "Answer" or "Response" to Clerk of the Superior Court, or electronically file your Answer through one of Arizona's approved electronic filing systems at <http://www.azcourts.gov/efilinginformation>. Mail a copy of your "Response" or "Answer" to the other party at the address listed on the top of this Summons. Note: If you do not file electronically you will not have electronic access to the document in this case.

3. If this “Summons” and the other court papers were served on you by a registered process server or the Sheriff, within the State of Arizona, your “Response” or “Answer” must be filed within TWENTY (20) CALENDAR DAYS from the date you were served, not counting the day you were served. If this “Summons” and the other papers were served on you by a registered process server or the Sheriff outside the State of Arizona, your Response must be filed within THIRTY (30) CALENDAR DAYS from the date you were served, not counting the day you were served. Service by a registered process server or the Sheriff is complete when made. Service by Publication is complete thirty (30) days after the date of the first publication.
4. You can get a copy of the court papers filed in this case from the Petitioner at the address at the top of this paper, or from the Clerk of the Superior Court.
5. Requests for reasonable accommodation for persons with disabilities must be made to the office of the judge or commissioner assigned to the case, at least ten (10) judicial days before your scheduled court date.
6. Requests for an interpreter for persons with limited English proficiency must be made to the office of the judge or commissioner assigned to the case at least ten (10) judicial days in advance of your scheduled court date.

SIGNED AND SEALED this Date: *January 13, 2025*

JEFF FINE
Clerk of Superior Court

By: *A. MARQUEZ*
Deputy Clerk



If you would like legal advice from a lawyer, contact Lawyer Referral Service at 602-257-4434 or <https://maricopabar.org>. Sponsored by the Maricopa County Bar Association.

Person Filing: Keith Beauchamp

Address (if not protected): 2800 North Central Avenue, Suite 1900

City, State, Zip Code: Phoenix, AZ 85004

Telephone: (602)381-5490

Email Address: kbeauchamp@cblawyers.com

Representing ☐ Self or ☒ Attorney for:

Lawyer's Bar Number: 012434, Issuing State: AZ

Clerk of the Superior Court
 *** Electronically Filed ***
 A. Marquez, Deputy
 1/13/2025 1:42:37 PM
 Filing ID 19154841

**SUPERIOR COURT OF ARIZONA
 IN MARICOPA COUNTY**

Case Number: **CV2025-001530**BLUE CROSS AND BLUE SHIELD OF ARIZONA, INC, et al.

Name of Plaintiff

SUMMONS

AND

CHANGE HEALTHCARE PRACTICE MANAGEMENT SOLUTION
 INC., et al.

Name of Defendant

WARNING: This is an official document from the court that affects your rights. Read this carefully.
 If you do not understand it, contact a lawyer for help.

FROM THE STATE OF ARIZONA TO: CHANGE HEALTHCARE SOLUTIONS, LLC

Name of Defendant

1. **A lawsuit has been filed against you.** A copy of the lawsuit and other court papers are served on you with this “*Summons*”.
2. If you do not want a judgment or order taken against you without your input, you must file an “*Answer*” or a “*Response*” in writing with the court and pay the filing fee. If you do not file an “*Answer*” or “*Response*” the other party may be given the relief requested in his/her Petition or Complaint. To file your “*Answer*” or “*Response*” take, or send, the “*Answer*” or “*Response*” to Clerk of the Superior Court, or electronically file your Answer through one of Arizona’s approved electronic filing systems at <http://www.azcourts.gov/efilinginformation>. Mail a copy of your “*Response*” or “*Answer*” to the other party at the address listed on the top of this Summons. Note: If you do not file electronically you will not have electronic access to the document in this case.

3. If this “Summons” and the other court papers were served on you by a registered process server or the Sheriff, within the State of Arizona, your “Response” or “Answer” must be filed within TWENTY (20) CALENDAR DAYS from the date you were served, not counting the day you were served. If this “Summons” and the other papers were served on you by a registered process server or the Sheriff outside the State of Arizona, your Response must be filed within THIRTY (30) CALENDAR DAYS from the date you were served, not counting the day you were served. Service by a registered process server or the Sheriff is complete when made. Service by Publication is complete thirty (30) days after the date of the first publication.
4. You can get a copy of the court papers filed in this case from the Petitioner at the address at the top of this paper, or from the Clerk of the Superior Court.
5. Requests for reasonable accommodation for persons with disabilities must be made to the office of the judge or commissioner assigned to the case, at least ten (10) judicial days before your scheduled court date.
6. Requests for an interpreter for persons with limited English proficiency must be made to the office of the judge or commissioner assigned to the case at least ten (10) judicial days in advance of your scheduled court date.

SIGNED AND SEALED this Date: *January 13, 2025*

JEFF FINE
Clerk of Superior Court

By: *A. MARQUEZ*
Deputy Clerk



If you would like legal advice from a lawyer, contact Lawyer Referral Service at 602-257-4434 or <https://maricopabar.org>. Sponsored by the Maricopa County Bar Association.

Person Filing: Keith Beauchamp

Address (if not protected): 2800 North Central Avenue, Suite 1900

City, State, Zip Code: Phoenix, AZ 85004

Telephone: (602)381-5490

Email Address: kbeauchamp@cblawyers.com

Representing ☐ Self or ☒ Attorney for:

Lawyer's Bar Number: 012434, Issuing State: AZ

Clerk of the Superior Court
*** Electronically Filed ***
A. Marquez, Deputy
1/13/2025 1:42:37 PM
Filing ID 19154840**SUPERIOR COURT OF ARIZONA
IN MARICOPA COUNTY**Case Number: **CV2025-001530**BLUE CROSS AND BLUE SHIELD OF ARIZONA, INC, et al.

Name of Plaintiff

SUMMONS

AND

CHANGE HEALTHCARE PRACTICE MANAGEMENT SOLUTION
INC., et al.

Name of Defendant

WARNING: This is an official document from the court that affects your rights. Read this carefully.
If you do not understand it, contact a lawyer for help.**FROM THE STATE OF ARIZONA TO: CHANGE HEALTHCARE TECHNOLOGIES, LLC**

Name of Defendant

1. **A lawsuit has been filed against you.** A copy of the lawsuit and other court papers are served on you with this "Summons".
2. If you do not want a judgment or order taken against you without your input, you must file an "Answer" or a "Response" in writing with the court and pay the filing fee. If you do not file an "Answer" or "Response" the other party may be given the relief requested in his/her Petition or Complaint. To file your "Answer" or "Response" take, or send, the "Answer" or "Response" to Clerk of the Superior Court, or electronically file your Answer through one of Arizona's approved electronic filing systems at <http://www.azcourts.gov/efilinginformation>. Mail a copy of your "Response" or "Answer" to the other party at the address listed on the top of this Summons. Note: If you do not file electronically you will not have electronic access to the document in this case.

3. If this “Summons” and the other court papers were served on you by a registered process server or the Sheriff, within the State of Arizona, your “Response” or “Answer” must be filed within TWENTY (20) CALENDAR DAYS from the date you were served, not counting the day you were served. If this “Summons” and the other papers were served on you by a registered process server or the Sheriff outside the State of Arizona, your Response must be filed within THIRTY (30) CALENDAR DAYS from the date you were served, not counting the day you were served. Service by a registered process server or the Sheriff is complete when made. Service by Publication is complete thirty (30) days after the date of the first publication.
4. You can get a copy of the court papers filed in this case from the Petitioner at the address at the top of this paper, or from the Clerk of the Superior Court.
5. Requests for reasonable accommodation for persons with disabilities must be made to the office of the judge or commissioner assigned to the case, at least ten (10) judicial days before your scheduled court date.
6. Requests for an interpreter for persons with limited English proficiency must be made to the office of the judge or commissioner assigned to the case at least ten (10) judicial days in advance of your scheduled court date.

SIGNED AND SEALED this Date: *January 13, 2025*

JEFF FINE
Clerk of Superior Court

By: *A. MARQUEZ*
Deputy Clerk



If you would like legal advice from a lawyer, contact Lawyer Referral Service at 602-257-4434 or <https://maricopabar.org>. Sponsored by the Maricopa County Bar Association.

1 Keith Beauchamp (012434)
2 Marvin C. Ruth (024220)
3 Malvika A. Sinha (038046)
4 Kelleen Mull (036517)
5 **COPPERSMITH BROCKELMAN PLC**
6 2800 North Central Avenue, Suite 1900
7 Phoenix, Arizona 85004
8 T: (602) 381-5490
9 F: (602) 224-6020
10 kbeauchamp@cblawyers.com
11 mruth@cblawyers.com
12 msinha@cblawyers.com
13 kmull@cblawyers.com

14 *Attorneys for Plaintiffs*

11
12 **SUPERIOR COURT OF ARIZONA**
13 **COUNTY OF MARICOPA**

14 BLUE CROSS AND BLUE SHIELD OF
15 ARIZONA, INC., an Arizona non-profit
16 corporation; and HEALTH CHOICE
ARIZONA, INC., an Arizona corporation,

17 Plaintiffs,

18 v.

19 CHANGE HEALTHCARE PRACTICE
20 MANAGEMENT SOLUTIONS, INC., a
21 Delaware corporation; CHANGE
22 HEALTHCARE TECHNOLOGIES, LLC, a
23 Delaware limited liability company;
CHANGE HEALTHCARE SOLUTIONS,
LLC, a Delaware limited liability company;
and CHANGE HEALTHCARE PAYER
PAYMENT INTEGRITY, LLC, a Delaware
limited liability company,

24 Defendants.

No. **CV2025-001530**

COMPLAINT

1 Plaintiffs Blue Cross and Blue Shield of Arizona, Inc. (“BCBSAZ”) and Health Choice
 2 Arizona, Inc. (“HCA”) relied on Defendants to provide services necessary to Plaintiffs’
 3 provision of health insurance and other products to more than two million Arizonans.
 4 Defendants were entrusted with highly confidential information from Plaintiffs—as well as
 5 personal health information of Plaintiffs’ members—on the condition that Defendants
 6 implement safeguards to protect that information. Defendants breached that trust by failing to
 7 employ even rudimentary precautions, resulting in disclosure of confidential data and tens of
 8 millions of dollars in damage to BCBSAZ. Plaintiffs filed this action because Defendants
 9 refuse to accept responsibility for the harms caused by their security failures.

10 **PARTIES, JURISDICTION & VENUE**

11 1. BCBSAZ is an Arizona nonprofit health insurance company with its principal
 12 place of business in Maricopa County, Arizona.

13 2. HCA is an Arizona for-profit corporation with its principal place of business in
 14 Maricopa County, Arizona.

15 3. Change Healthcare Practice Management Solutions, Inc. (“CHP”) is, on
 16 information and belief, a Delaware Corporation.

17 4. Change Healthcare Technologies, LLC (“CHTech”), Change Healthcare
 18 Solutions, LLC (“CHSolutions”), and Change Healthcare Payer Payment Integrity, LLC
 19 (“CHPayer”), are, on information and belief, Delaware limited liability companies. The
 20 Change Health entities are collectively referred to as “CHC”.

21 5. Each of the Defendants caused events to occur in Maricopa County out of which
 22 Plaintiffs’ claims arise. Further, Maricopa County is the county in which Plaintiffs reside.
 23 Venue is therefore proper in Maricopa County pursuant to A.R.S. § 12-401(1), (5).

24 6. This Court has jurisdiction pursuant to A.R.S. § 12-123.

25 7. Pursuant to Rule 26.2 of the Arizona Rules of Civil Procedure, Tier 3 is
 26 appropriate for this case based upon its complexity and the amount in controversy.

INTRODUCTION

8. BCBSAZ provides health insurance and related services to more than two million Arizona customers. It does so through a variety of products, including a statewide Preferred Provider Organization network, local Health Maintenance Organization networks, Medicare Advantage plans, and individual health plans, including plans offered on the federal healthcare exchange through the Affordable Care Act (“ACA”).

9. HCA provides health plan services to qualified Medicaid and Dual Eligible Special Needs (“D-SNP”) members through contracts with the Arizona Health Care Cost Containment System (“AHCCCS”) and the Centers for Medicare and Medicaid Services (“CMS”).

10. CHC is one of the largest health payment processing companies in the world. Among other things, it acts as a clearinghouse for claims processing, and upon information and belief, processes 15 billion medical claims each year, accounting for nearly 40 percent of all claims. As the nation’s largest clearing house, CHC receives claims from medical practices, processes and verifies them, and sends them to insurers for payment; checks for errors and missing information; tracks the status of those claims; and verifies patient insurance eligibility, among other tasks.

11. CHC is a subsidiary of UnitedHealth Group, the largest healthcare insurer in the United States.

12. CHC provided critical clearinghouse, risk adjustment, and other health insurance related services to BCBSAZ and HCA for many years pursuant to multiple agreements. In doing so, it received significant confidential information from BCBSAZ and HCA, including electronic Personal Health Information (“PHI”) of many of BCBSAZ’s and HCA’s members.

13. CHC agreed that it would implement safeguards to protect this confidential information, and that it would take no less than a reasonable degree of care to prevent any unauthorized use, access or disclosure of that confidential information.

14. CHC further represented to BCBSAZ that many of these safeguards, including baseline security protocols such as Multi-factor Authentication, were already in place.

15. Despite its promises, CHC failed to implement even the most rudimentary security safeguards.

16. On February 12, 2024, cybercriminals accessed a portal that, contrary to CHC's policy and industry standards, did not employ multi-factor authentication ("MFA"). After spending more than a week rummaging through CHC's data undetected, the criminals employed ransomware that not only encrypted the information on CHC's main systems, but also CHC's backups.

17. As a result, by February 21, 2024, CHC was unable to provide any contractually obligated services to BCBSAZ and HCA, leaving BCBSAZ and HCA scrambling to find alternatives, costing BCBSAZ and HCA millions through higher costs and delays. Moreover, now unable to access its own confidential information, BCBSAZ was also unable to process claims, timely provide data to regulators, or audit prior payments, resulting in millions of dollars of additional damages.

18. Months after the cyber-attack, with CHC still unable to cure its breaches, BCBSAZ terminated most of its contracts with CHC.

GENERAL ALLEGATIONS

I. CHC CONTRACTS WITH BCBSAZ TO PROVIDE VARIOUS SERVICES; EACH CONTRACT REQUIRES PROTECTION OF CONFIDENTIAL INFORMATION

A. The BPaaS Agreement

19. BCBSAZ and CHP and CHTech were parties to a Master Services Agreement effective February 15, 2019, which included eleven (11) Statements of Work (the "SOWs"), together with a Business Associate Agreement ("BAA") (collectively, the "BPaaS Agreement").

1 20. Pursuant to the BPaaS Agreement, CHP and CHTech were obligated to provide
2 BCBSAZ with certain services (collectively, the “BPaaS Services”), including, but not limited
3 to: (i) clearinghouse services (claim processing, member management, etc.); (ii) management
4 of Medicare enrollments and membership; (iii) risk adjustment services specific to BCBSAZ’s
5 Medicare Advantage population, which adjusts the amounts Medicare Advantage
6 organizations may be required to pay or receive based on the expected healthcare costs of their
7 patient population; and (iv) risk adjustment services specific to BCBSAZ’s Medicaid
8 population

9 21. In addition to those services and pursuant to the BPaaS Agreement, CHP and
10 CHTech also built BCBSAZ’s claims system software, Payor Connectivity Services (“PCS”).
11 PCS is a claims administration, routing and first-pass adjudication system created by CHP and
12 CHTech for BCBSAZ to consolidate and manage inbound and outbound transaction streams.

13 22. BCBSAZ used PCS to bring a significant portion of electronic claims into its
14 HealthRules Payer (“HRP”) system. HRP is a core administrative processing system that
15 provides a unified platform to manage financial, clinical, and administrative operations.

16 23. The PCS system built and maintained by CHP and CHTech for BCBSAZ was
17 the primary means by which data was supplied to the HRP system used by BCBSAZ for claims
18 processing, regulatory compliance, and other critical functions.

19 24. To facilitate this broad array of services, BCBSAZ provided CHP and CHTech
20 with “Confidential Information,” which is defined by the BPaaS Agreement as any:

21 nonpublic information . . . which by its nature should reasonably be understood
22 to be confidential, including, but not limited to, information relating to: . . . the
23 identity of BCBSAZ’s current and prospective members or vendors; . . .
24 personally identifying or confidential information of BCBSAZ’s and its
25 Affiliates’ respective personnel, members, customers, or providers . . . and
26 information received from others that a Party is obligated to treat as confidential.

1 25. Pursuant to the BPaaS Agreement, CHP and CHTech agreed that they would
2 “keep in confidence all Confidential Information” received from BCBSAZ.

3 26. CHP and CHTech further agreed to “safeguard the Confidential Information
4 from unauthorized use, access or disclosure using at least the degree of care it uses to protect
5 its similarly sensitive information and in no event less than a reasonable degree of care”
6 *Id.* Finally, CHP and CHTech agreed that “to the extent BCBSAZ’s Confidential Information
7 includes any protected health information (“PHI”), the Parties agree to comply with the terms
8 of the [BAA], which provides additional terms relating to PHI.” *Id.*

9 **1. The BPaaS Agreement imposes risk mitigation obligations on CHC**

10 27. Section 12.1 of the BPaaS Agreement provides that CHP and CHTech would
11 ensure continued performance of their services in the event of a disaster and references and
12 incorporates CHC’s Disaster Recovery Plan.

13 28. Specifically, Section 12.1 of the BPaaS Agreement states:

14 If, despite [CHC’s] efforts, [CHC] is unable to perform disaster recovery
15 and is therefore unable to continue or recommence performance, within 72 hours
16 of the occurrence of the disaster, of the Services that are essential to the
17 continued operations of BCBSAZ’s business, BCBSAZ will be entitled to pursue
18 all remedies available to BCBSAZ at law, in equity and under this Agreement.
If Contractor is unable to recommence non-essential Services within 10 days
following such 72 hour period, BCBSAZ will be entitled to pursue all remedies
available to BCBSAZ at law, in equity and under this Agreement.

19 29. In turn, CHP and CHTech represented to BCBSAZ in the referenced Disaster
20 Recovery Plan that “extensive procedures have been developed to support the resumption of
21 time-sensitive business operations and functions in the event of a disruption Change
22 Healthcare is committed to supporting company resumption and recovery efforts at its primary
23 facilities and alternate facilities, if required.”

24 30. CHP and CHTech further represented to BCBSAZ that “all critical data, system
25 software, applications, and databases are stored in a secure off-site location and are accessible
26 immediately following the disaster or significant adverse event.” *Id.* at 12.

1 **2. The BPaaS Agreement obligates CHC to implement security policies**
 2 **for PHI that it receives or transmits**

3 31. In the Delegation Addendum to the BPaaS Agreement, CHP and CHTech
 4 represented and agreed to implement privacy and security policies and procedures for any PHI
 5 or personally identifiable information (“PII”) that they create, receive, store, or transmit.

6 32. As further represented and agreed by CHC in the Delegation Addendum, those
 7 “policies and procedures must, at minimum, (a) satisfy the requirements of applicable law, (b)
 8 protect electronic PII and PHI through encryption or its comparable equivalent, (c) address the
 9 protection of PII and PHI in connection with ephemeral messaging solutions, if applicable, and
 10 (d) address cloud storage and social media applications, if applicable.” *Id.*

11 **3. The Business Associate Agreement imposes further security**
 12 **obligations on CHC to protect Confidential Information received**
 from BCBSAZ

13 33. CHP entered into the BAA with BCBSAZ.

14 34. In signing the BAA, CHP agreed to additional mandatory safeguards specific to
 15 PHI.

16 35. CHP represented and agreed that it would “develop, implement, maintain and
 17 use appropriate administrative, technical, and physical safeguards (“Safeguards”) to protect
 18 the privacy of [BCBSAZ’s] PHI.” CHP further represented and agreed that “[t]he Safeguards
 19 must reasonably protect the privacy of [BCBSAZ’s] PHI from any intentional or unintentional
 20 use or disclosure in violation of the Privacy Rule, 45 C.F.R. Part 164, Subpart E and this BAA
 21”

22 36. CHP further represented and agreed to “maintain and use *appropriate*
 23 *administrative, technical and physical safeguards, in compliance with the HIPAA Security*
 24 *Rule, standard business practices, any other applicable regulations governing privacy and*
 25 *security* . . . to preserve the integrity, availability and confidentiality of, and to prevent non-

1 permitted or violating use or disclosure of, Electronic PHI created or received for or from
2 [BCBSAZ].”

3 **B. The Diagnosis Related Group Agreement**

4 37. A Diagnosis Related Group or “DRG” is a classification system that groups
5 inpatient hospital stays for purposes of payment. Patients are grouped based on, among other
6 things, their diagnosis, medical conditions, age, sex, medical procedure, and the resources
7 required for their treatment. Based on those factors, the DRG system then sets different
8 payment rates for those patient groupings based on severity of illness, risk of mortality or co-
9 morbidity, and treatment difficulty.

10 38. A DRG audit is a process that verifies that the hospital receiving payment from
11 the insurer has properly billed all diagnoses and procedure codes in accordance with DRG
12 coding guidelines, and that the billing codes submitted are consistent with the medical
13 records. The goal of such an audit is to ensure that medical records are accurately reflected in
14 diagnostic and procedure codes, and that hospitals are appropriately reimbursed for services
15 rendered.

16 39. CHC provided DRG audit and recovery services (the “DRG Services”) to
17 BCBSAZ pursuant to an agreement styled as the November 1, 2007 Solution Order between
18 BCBSAZ and CHPayer effective September 27, 2022 (the “Solution Order”). The Solution
19 Order is subject to and incorporated into a 2007 License Agreement between BCBSAZ and
20 CHTech (the “License Agreement”).

21 40. The License Agreement was originally entered into between McKesson
22 Technologies, LLC and BCBSAZ. CHTech was the successor-in-interest to McKesson
23 Technologies for purposes of the DRG Agreement as set forth in a November 1, 2007 Contract
24 Supplement.

25 41. BCBSAZ utilized the DRG Services to ensure it was making proper payments
26 to hospitals for inpatient stays and obtaining reimbursements for prior overcharges.

1 42. In order for CHPayer and CHTech to provide the DRG Services, BCBSAZ was
2 obligated to “provide CHC with the necessary Customer Data to perform the Services,” which
3 data included Confidential Information, defined to include BCBSAZ’s “medical records, and
4 other information that is marked confidential or which the receiving party should reasonably
5 know to be confidential.” Thus, patient claims data and PHI are defined as “Confidential
6 Information” for purposes of the DRG Agreement.

7 43. The DRG Agreement obligates CHPayer and CHTech to protect BCBSAZ’s
8 “Confidential Information.” Specifically, they must “use all reasonable care in handling and
9 securing the other party’s Confidential Information” and must “employ all security measures
10 ordinarily used for its own proprietary information of similar nature.” *Id.* at § 6.2.

11 **C. The HCA Agreement**

12 44. HCA and CHSolutions are parties to the WebMD Business Services Payer
13 Agreement, effective May 19, 2005 (the “HCA Agreement”, together with the BPaaS
14 Agreement and the DRG Agreement, the “Agreements”).

15 45. Under the HCA Agreement, CHSolutions was obligated to provide
16 clearinghouse services to HCA, including (i) core claim services, (ii) imaging and Electronic
17 Data Interchange services, (iii) processing, production, and mailing of member Explanation of
18 Benefits and provider checks and remittances, (iv) claim management services, and (v) “per
19 member per month” revenue cycle management services.

20 46. As with the BPaaS Agreement and the DRG Agreement, the HCA Agreement
21 requires that CHSolutions use “no less than reasonable care” to protect HCA’s Confidential
22 Information, defined to include “individually identifiable medical or financial information.”
23 *Id.* at § C.2.

II. CHC WAS REQUIRED TO IMPLEMENT REASONABLE SECURITY MEASURES AS SET FORTH IN THE HIPAA SECURITY RULE INCORPORATED INTO THE AGREEMENTS

47. In addition to CHC's express written obligations to safeguard and protect Confidential Information from unauthorized use and access, the Agreements also required that CHC implement and maintain reasonable security measures to protect the integrity and confidentiality of BCBSAZ's Confidential Information.

48. Further, the HIPAA Security Rule, which is expressly referenced and incorporated in the BPaaS Agreement, establishes national standards to protect electronic health information ("ePHI") that is created, received, used, or maintained by covered entities and business associates such as CHC.

49. The HIPAA Security Rule thus sets forth, at a minimum, the reasonable security measures CHC should maintain to ensure that BCBSAZ's Confidential Information remains confidential and free from unauthorized access or use.

50. The HIPAA Security Rule requires regulated entities to meet certain administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI, including safeguards with respect to access, control, authentication, workstation security, and device controls. *See* 45 C.F.R. §§ 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards).

51. The BAA likewise provides that CHC would "develop, implement, maintain and use appropriate administrative, technical, and physical safeguards ("Safeguards") to protect the privacy of [BCBSAZ's] PHI."

52. The HIPAA Security Rule also contains implementation specifications with additional detail on compliance with the foregoing safeguards. These implementation specifications are either required (meaning they are mandatory) or addressable (meaning that regulated entities must perform an assessment to determine whether each addressable

1 implementation specification is a reasonable and appropriate safeguard to implement in the
2 regulated entity's environment). *See, e.g.*, 45 C.F.R. §§ 164.308, 164.310, 164.312.

3 53. Under the HIPAA Security Rule, in deciding which security measures to
4 implement, companies must consider their own size, complexity, capabilities, technical
5 infrastructure, cost of security measures, and the probability and criticality of potential risks to
6 electronic health information. 45 C.F.R. § 164.306(b).

7 54. Given CHC's status as the largest health payment processing company in the
8 United States, charged with processing voluminous amounts of PHI and other confidential
9 information found in its systems, CHC should have implemented all of the relevant security
10 measures.

11 55. The industry standard for security frameworks to implement the HIPAA Security
12 Rule is the NIST 800-66, a publication by the National Institute of Standards and Technology.

13 **A. Administrative Safeguards**

14 56. The HIPAA Security Rule requires covered health care companies such as CHC
15 to implement administrative safeguards to protect data and confidential information, which are
16 subject to further standards. *See* 45 C.F.R. §§ 164.308.

17 57. For example, the Security Rule requires a covered entity to meet Contingency
18 Plan Standards, whereby CHC establishes and implements policies and procedures for
19 responding to vandalism, system failures, and other emergencies. 45 C.F.R. § 164.308(a)(7)(i).

20 58. To comply with this standard, CHC must have data backup and disaster recovery
21 plans, and is required to "[e]stablish and implement procedures to create and *maintain*
22 *retrievable exact copies of electronic protected health information*," 45 C.F.R. §
23 164.308(a)(7)(ii)(A).

24 59. CHC was also required to "[e]stablish (and implement as needed) procedures to
25 restore any loss of data." 45 C.F.R. § 164.308(a)(7)(ii)(B) (emphasis added).

1 60. The NIST likewise required CHC to have in place procedures that enable the
2 continuation of critical processes. *See* NIST SP 800-66 § 5.1.7.

3 61. CHC must also meet the Security Management Process Standard. That standard
4 requires that the covered entity “[i]mplement policies and procedures to prevent, detect,
5 contain, and correct security violations.” 45 C.F.R. § 164.308(a)(1)(i). To comply with this
6 standard, covered entities such as CHC must “[i]mplement procedures to regularly review
7 records of information system activity, such as *audit logs, access reports, and security*
8 *incident tracking reports.*” C.F.R. § 164.308(a)(1)(ii)(D) (emphasis added).

9 **B. Physical Safeguards**

10 62. Covered entities must also implement and maintain physical safeguards, which
11 are subject to further standards. 45 C.F.R. § 164.310 (physical safeguards).

12 63. For example, CHC must meet the Workstation Security Standard, which requires
13 that the entity “[i]mplement physical safeguards for all workstations that access electronic
14 protected health information, to restrict access to authorized users.” 45 C.F.R. § 164.310(c).
15 This includes: (i) identifying all methods of physical access to workstations and devices,
16 including remote access; (ii) analyzing the risks associated with each type of access, and (iii)
17 implementing physical safeguards—*such as device encryption and multifactor*
18 *authentication*—to minimize the possibility of inappropriate access to ePHI through
19 computing devices. NIST 800-66 at 5.2.3., Table 19 (p. 61) (emphasis added).

20 **C. Technical Safeguards**

21 64. CHC, as a covered entity, must also implement and maintain technical
22 safeguards, which are subject to further standards. 45 C.F.R. § 164.312 (technical safeguards).

23 65. For example, CHC must meet the Access Control Standard, which requires,
24 among other things, that it “[i]mplement technical policies and procedures for electronic
25 information systems that maintain electronic protected health information to allow access only
26 to those persons or software programs that have been granted access rights” Further, to

1 comply with this standard, CHC must establish, and implement as needed, emergency access
2 procedures for obtaining necessary ePHI during an emergency. 45 C.F.R. § 164.312(a)(2)(ii);
3 *see* NIST 800-66 at 5.3.1., Table 21 (p. 67).

4 66. CHC must also meet the Person or Entity Authentication Standard, which
5 requires, among other things, that the entity “[i]mplement procedures to verify that a person or
6 entity seeking access to electronic protected health information is the one claimed.” 45 C.F.R.
7 § 164.312(d). Per the NIST, this includes: (i) determining authentication applicability to
8 current systems and applications, including for remote access points; (ii) evaluating available
9 authentication options (including MFA solutions “when the risk of ePHI is sufficiently high.”);
10 and (iii) selecting and implementing authentication options based on a risk assessment analysis.
11 NIST 800-66 at 5.3.4., Table 24 (p. 73).

12 67. Notably, the NIST identifies remote access as an access point that “poses high
13 risk” and may be particularly appropriate for multifactor authentication. *Id.* at 74.

14 68. Further, CHC must meet the Transmission Security Standard, which requires,
15 among other things, that the entity “[i]mplement technical security measures to guard against
16 unauthorized access to electronic protected health information that is being transmitted over
17 an electronic communications network.” 45 C.F.R. § 164.312(e)(1). Regulated entities must
18 assess whether it is reasonable and appropriate to, among other things, “[i]mplement an
19 electronic mechanism to encrypt [ePHI] whenever deemed appropriate.” 45 C.F.R.
20 § 164.312(e)(2)(ii). Per NIST, covered entities should, among other things, identify any
21 possible sources that may be able to intercept or modify information, identify scenarios and
22 pathways that may put ePHI at a high level of risk, and assess whether encryption is needed to
23 effectively prevent unauthorized access. NIST 800-66 at 5.3.5., Table 25 (p. 75-76).

1 **III. CHC MAKES ADDITIONAL REPRESENTATIONS TO BCBSAZ**
2 **REGARDING ITS ALLEGED SECURITY MEASURES**

3 69. In addition to the contractual promises described above, CHC made multiple
4 additional representations to BCBSAZ regarding its allegedly robust security measures and
5 protocols that would purportedly protect BCBSAZ's Confidential Information.

6 70. CHC's 2021 Information Security Program Overview, for example, boasts of a
7 strong cyber threat management program, including a team that "[m]aintains a comprehensive
8 incident response plan to assess and respond to information security-related events,"
9 "maintains awareness of the cyber threat landscape;" and "[i]dentif[ies] potential, existing and
10 emerging threats to [CHC], its customers, and the healthcare industry.

11 71. CHC's Information Security Program Overview further touts a customer security
12 assurance program that "provides transparency and relevant information to Change
13 Healthcare's clients of our information security program and practices to give assurance that
14 information under our care is properly protected and complies with appropriate regulations and
15 contract commitments." *Id.* at 9.

16 72. CHC also made representations to BCBSAZ regarding its use of MFA.

17 73. MFA is a two-step verification system that requires users to provide more than
18 just a password to access an account, and which prompts them to provide a second form of
19 authentication.

20 74. MFA is a widely and commonly used security measure.

21 75. Use of MFA has long been standard practice in the healthcare industry.

22 76. Use of MFA should be a critical baseline practice for CHC, which is both a
23 subsidiary of the nation's largest private health insurer, and the largest data clearinghouse in
24 the nation.

25 77. CHC touted its alleged MFA policies in external-facing communications, such
26 as its 2021 Information Security Program Overview, *wherein CHC stated that the company*

1 *requires MFA “to remotely access confidential data, and where a higher level of security is*
2 *needed to protect high risk assets.”* (emphasis added)

3 78. CHC further represented to BCBSAZ that “*MFA is required to remotely access*
4 *the private-trusted Change Healthcare network* from a public or untrusted network. In order
5 to remotely access the network, workers must access the network using VPN or a desktop
6 solution such as . . . Citrix. *These access methods are integrated with MFA to ensure the*
7 *validity of worker identities.”* *Id.* (emphasis added).

8 79. Additionally, in its response to BCBSAZ’s 2023 Company Questionnaire, CHC
9 answered “Yes” to the question: “Does your company require multi-factor authentication for
10 high-risk environments?”

11 80. CHC represented to BCBSAZ that “*security for remote access [is] implemented*
12 *using network segmentation and virtual desktop infrastructure protected by MFA”* *Id.*
13 (emphasis added)

14 81. CHC also made additional representations to BCBSAZ regarding its use of
15 backup data to protect BCBSAZ’s data.

16 82. Again, CHC represented and acknowledged through its Information Security
17 Program Overview that “[d]ata backups are required to ensure recovery from data loss and/or
18 corruption,” and that CHC’s data resides not only at its two primary data centers in Tennessee,
19 but also at a “series of secondary data centers across the United States, and in the Amazon,
20 Microsoft, and Google Cloud environments.”

21 83. CHC also represented that it uses an enterprise backup software to manage all
22 backup operations, that it has a “dedicated backup network,” and that it utilizes off-site storage
23 and stored media retrieval. *Id.* at 41-42.

1 **IV. CHC'S DEFICIENT SECURITY ALLOWS A THIRD PARTY TO STEAL**
2 **BCBSAZ'S CONFIDENTIAL INFORMATION, CAUSING TENS OF**
3 **MILLIONS OF DOLLARS IN DAMAGES TO BCBSAZ**

4 84. On February 12, 2024, a ransomware group accessed CHC's systems using
5 stolen or compromised credentials (the "Cyber Event").

6 85. According to testimony by UnitedHealth Group CEO Andrew Witty to the
7 United States Congress, the ransomware group, believed to go by the name AlphV, used
8 compromised credentials to "remotely access a Change Healthcare Citrix portal, an application
9 used to enable remote access to desktops." After operating undetected in CHC's systems for
10 nine days, AlphV exfiltrated data and deployed ransomware that encrypted CHC's systems,
11 including its backup systems.

12 86. AlphV accessed and used BCBSAZ's Confidential Information.

13 87. The Cyber Event rendered BCBSAZ's Confidential Information, including
14 confidential patient data and claim information, inaccessible.

15 88. CHC did not learn of the Cyber Event until February 21, 2024, at which point
16 CHC disclosed to BCBSAZ that its systems had been compromised.

17 89. CHC instructed BCBSAZ and HCA to disconnect all interfaces and connections
18 between BCBSAZ, HCA, and CHC.

19 90. CHC stopped providing services to BCBSAZ under the BPaaS Agreement, HCA
20 Agreement, and DRG Agreement.

21 91. CHC has never resumed the provision of services to BCBSAZ under the BPaaS
22 Agreement or the DRG Agreement.

23 92. BCBSAZ was unable to access its own claims data to take some of those services
24 in-house, and was unable to utilize its own HRP claims processing system because the PCS
25 software developed and maintained by CHC was compromised as a result of the Cyber Event.

26 93. As a result of the Cyber Event, CHC's subsequent inability and refusal to provide
services under the Agreement, and BCBSAZ's inability to process claims on its HRP system,

1 BCBSAZ was forced to search for and retain alternative vendors who could attempt to provide
2 the claims processing services critical to its business.

3 94. As a result of CHC's failure, refusal, and inability to provide services under the
4 Agreements, and its failure to maintain confidentiality as required by the Agreements,
5 BCBSAZ and HCA have incurred significant damages, including: (i) hiring new vendors at a
6 premium to provide the services CHC was obligated to provide under the BPaaS and HCA
7 Agreements, (ii) diverting existing employees from other critical projects to execute this rapid
8 change in an effort to avoid catastrophic harm to its members and to providers, and (iii) losing
9 out on revenue streams that were dependent on CHC's services.

10 95. CHC failed to implement the robust cyber security practices it was obligated to
11 implement pursuant to the Agreements, and which it had falsely touted in its external-facing
12 communications to BCBSAZ.

13 **A. CHC Failed to Implement Multi-Factor Authentication**

14 96. In May 2024, UnitedHealth Group CEO Andrew Witty admitted in
15 Congressional testimony that the Cyber Event occurred because a remote access CHC Citrix
16 portal did not require MFA.

17 97. Mr. Witty further admitted that CHC used outdated systems that lacked MFA
18 and needed replacement.

19 98. Specifically, Mr. Witty testified that:

20 Cybercriminals entered a Change Health Care portal, exfiltrated data, and
21 on February 21, deployed ransomware. The portal they accessed was not
22 protected by multifactor authentication . . . I'm very disappointed and frustrated
23 that this particular server did not have MFA installed. Change Healthcare came
24 into our group a little over a year and a half ago. We've been upgrading their
25 technology since we acquired it . . . [Change Healthcare was] established 2007,
26 but some of the legacy systems in that company go back 40 years. We've been

working to improve those, and unfortunately we have discovered a server which was not covered by MFA, and as a result . . . was exploited.¹

99. Mr. Witty further testified:

We're continuing to investigate as to exactly why MFA was not on that particular server. It clearly was not. . . . For some reason, which we continue to investigate, this particular server did not have MFA on it.²

100. This testimony confirms that CHC's representation to BCBSAZ that Citrix access points "are integrated with MFA to ensure the validity of worker identities" was false.

101. CHC's failure to ensure that MFA was required to access its portals violated, among other things, (i) the Security Management Process standard, which requires implementation of policies and procedures "to prevent, detect, contain, and correct security violations;" (ii) the Workplace Security standard, which requires implementation of physical safeguards for all workstations accessing ePHI; (iii) the Access Control standard, which requires implementation of technical policies and procedures for systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights; and (iv) the Person or Entity Authentication standard, which requires implementation of procedures to "verify that a person or entity seeking access to electronic protected health information is the one claimed." *See* 45 C.F.R. §§ 164.308(a)(1)(i), 164.310(c), 164.312(a)(2)(ii), 164.312(d).

102. Given CHC's size and role in the marketplace, and the type and volume of information it stored, it was required to use MFA pursuant to the policies and procedures set out in the foregoing paragraph. *See, e.g.*, NIST 800-66 at 5.3.4., Table 24 (p. 73).

¹ CBS News, UnitedHealth CEO Andrew Witty testifies about cyberattack (May 1, 2024) *available at* https://www.youtube.com/watch?v=vjQAcWy1_dQ [at 11:48-12:03, 1:45:45-1:46:14]

² Energy & Commerce Committee, What We Learned: Change Healthcare Cyber Attack (May 3, 2024) *available at* <https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack>.

B. CHC Failed to Properly Back Up BCBSAZ's data

103. CHC failed to back up BCBSAZ's data in a secure manner.

104. The Cyber Event initially prevented CHC from accessing *both* its primary *and* backup systems, which were immobilized and unusable for weeks after the cyberattack.

105. CHC's inability to access its primary and backup systems left BCBSAZ without access to critical claims data for months.

106. As a result of this lack of access, BCBSAZ was unable to process claims or report information regarding those claims.

107. CHC's data backup policies were not reasonable and violated, among other things, the Security Rule's "Data Backup Plan" standard, which requires covered entities to "[e]stablish and implement procedures to create and maintain retrievable exact copies of electronic protected health information." 45 C.F.R. § 164.308(7)(ii)(A).

108. Although the BPaaS Agreement and BAA require that CHC maintain administrative, technical, and physical safeguards to secure BCBSAZ's data in multiple locations, the cyber criminals were able to encrypt, and thereby lockdown, the primary and backup data locations, thereby rendering the purported "backup" of CHC's data useless.

C. CHC Failed to Deploy Robust Anti-Malware Software

109. Mr. Witty testified that the threat actor was able to move laterally within CHC's systems for nine days undetected, exfiltrating data before deploying the ransomware attack.

110. Robust anti-virus and anti-malware software would have enabled CHC to detect the lateral movement and prevent the attack and subsequent encryption of BCBSAZ Confidential Information, or at least minimize the harm.

111. CHC's lack of proper security systems violated, among other things, the Security Management Process Standard, which requires that entities such as CHC "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations." 45 C.F.R. § 164.308(a)(1)(i). *See also* 45 C.F.R. § 164.308(a)(1)(ii)(D) (procedures should be implemented

1 to “regularly review records of information system activity, such as audit logs, access reports,
2 and security incident tracking reports.”)

3 **D. CHC Failed to Implement Reasonable Security Procedures As Agreed**

4 112. The Agreements required CHC to exercise reasonable care, comply with the
5 HIPAA Security Rule and meet industry standards. For example:

- 6 • the BPaaS Agreement required CHC to “safeguard the Confidential
7 Information from unauthorized use, access or disclosure using at least the
8 degree of care it uses to protect its similarly sensitive information ***and in no
event less than a reasonable degree of care . . .***” (emphasis added).
- 9 • the BAA required CHC to “maintain and ***use appropriate administrative,
10 technical and physical safeguards, in compliance with the HIPAA Security
11 Rule, standard business practices, [and] any other applicable regulations***
governing privacy and security . . . to preserve the integrity, availability and
12 confidentiality of, ***and to prevent non-permitted use or violating use or
disclosure of, Electronic PHI . . .***” (emphasis added).
- 13 • The HCA Agreement required that CHC use “***no less than reasonable care***” to
14 protect HCA’s Confidential Information. (emphasis added)
- 15 • The DRG License Agreement required that CHC “***use all reasonable care*** in
16 handling and securing” BCBSAZ’s Confidential Information. (emphasis added)

17 113. CHC failed to exercise reasonable care, failed to comply with the HIPAA
18 Security Rule, and failed to meet industry standards in safeguarding BCBSAZ Confidential
19 Information.

20 114. Among other things, CHC failed to use MFA; failed to update antiquated
21 hardware and software notwithstanding the enormous volume of sensitive data it controlled;
22 failed to employ anti-malware software, thereby allowing the criminals to spend more than a
23 week infiltrating its systems undetected; and failed to maintain secure backup files.

24 115. These failures contradict CHC’s written policies and representations to
25 BCBSAZ and fall well below industry and regulatory standards.

1 **V. BCBSAZ GIVES NOTICE OF CHC’S VARIOUS BREACHES; CHC FAILS TO**
2 **CURE**

3 **A. BCBSAZ Gives Notice of CHC’s Material Breaches of the BPaaS**
4 **Agreement and Later Terminates the Agreement for Cause**

5 116. On March 7, 2024, BCBSAZ gave notice to CHC that it was in breach of the
6 BPaaS Agreement by (i) failing to provide BPaaS Services after February 21, 2024 as required
7 by the BPaaS Agreement and relevant SOWs; (ii) failing to resume providing BPaaS Services
8 considered essential to BCBSAZ’s continued operations within 72 hours of the Cyber Event
9 as required by Section 12 of the BPaaS Agreement; and (iii) violating the representation and
10 warranty in Section 9.2(f) of the BPaaS Agreement that the BPaaS Services would be available
11 in accordance with the Service Level Agreement in the applicable SOWs (the “First Breach
12 Notice”).

13 117. CHC did not respond to the First Breach Notice.

14 118. CHC did not resume providing the BPaaS Services after receiving the First
15 Breach Notice or otherwise cure its breaches.

16 119. On May 1, 2024, BCBSAZ gave notice to CHC of additional BPaaS Agreement
17 breaches, including CHC’s failure to maintain administrative, technical, and physical
18 safeguards in compliance with the HIPAA Security Rule and as required by the BAA (the
19 “Second Breach Notice”).

20 120. Again, CHC did not respond to the Second Breach Notice.

21 121. Again, CHC did not resume providing the BPaaS Services after receiving the
22 Second Breach Notice or otherwise cure its breaches.

23 122. On May 1, 2024 BCBSAZ provided CHC written notice that it was terminating
24 the BPaaS Agreement and all active SOWs for cause, pursuant to Section 11.2(a) of the BPaaS
25 Agreement.
26

B. BCBSAZ Gives Notice of CHC's Material Breaches of the DRG Agreement

123. On June 10, 2024, BCBSAZ gave notice to CHC that it was in material breach of the DRG Agreement by failing to provide any of the DRG Services after the Cyber Event (the "DRG Breach Notice").

124. Pursuant to the DRG Agreement, CHC had 60 days to cure the breach.

125. CHC failed to cure its breach under the DRG Agreement.

126. CHC failed and refused to resume providing the DRG Services.

127. On September 30, 2024, BCBSAZ terminated the DRG Agreement.

C. BCBSAZ Gives Notice of CHC's Breaches of the HCA Agreement

128. On March 8, 2024, HCA gave notice to CHC that it was in breach of the HCA Agreement for failing, among other things, to provide: (i) core claim services, (ii) imaging and EDI services, (iii) processing, production, and mailing of member Explanation of Benefits and provider checks and remittances, (iv) claim management services, and (v) "per member per month" revenue cycle management services.

129. As with the BPaaS Breach Notice and the DRG Breach Notice, CHC did not respond.

130. CHC did resume providing limited printing services under the HCA Agreement.

131. CHC did not cure any of its other breaches under the HCA Agreement.

D. CHC Admits a HIPAA Breach

132. In a June 20, 2024 public statement, CHC conceded (i) that the Cyber Event was a "Breach" under HIPAA and (ii) that PHI (necessarily including BCBSAZ and HCA's Confidential Information), had been inappropriately accessed and exfiltrated.

**COUNT I
BREACH OF THE BPAAS AGREEMENT
(Against CHP and CHTech)**

133. Plaintiffs incorporate by reference each and every allegation contained in the preceding paragraphs as though fully set forth herein.

1 143. BCBSAZ is also entitled to its costs, expenses and fees, including, without
2 limitation, attorneys' fees and costs incurred in enforcing and collecting the obligations
3 described in this Complaint, pursuant to A.R.S. §§ 12-341 and 12-341.01, and any applicable
4 contractual provisions.

5 **COUNT III**
6 **BREACH OF THE DRG AGREEMENT**
7 **(Against CHPayer and CHTech)**

8 144. Plaintiffs incorporate by reference each and every allegation contained in the
9 preceding paragraphs as though fully set forth herein.

10 145. The DRG Agreement is a valid and enforceable agreement between BCBSAZ,
11 CHPayer, and CHTech.

12 146. CHPayer and CHTech have breached their obligations under the DRG
13 Agreement by, among other things, (i) failing and refusing to provide the DRG Services and
14 (ii) allowing unauthorized access to and use of BCBSAZ's Confidential Information, as set
15 forth above.

16 147. BCBSAZ has been damaged by CHPayer and CHTech's breaches of their
17 obligations under the DRG Agreement in an amount to be proven at trial.

18 148. BCBSAZ is also entitled to its costs, expenses and fees, including, without
19 limitation, attorneys' fees and costs incurred in enforcing and collecting the obligations
20 described in this Complaint, pursuant to A.R.S. §§ 12-341 and 12-341.01, and any applicable
21 contractual provisions.

22 **COUNT IV**
23 **BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING IN**
24 **CONNECTION WITH DRG AGREEMENT**
25 **(Against CHPayer and CHTech)**

26 149. Plaintiffs incorporate by reference each and every allegation contained in the
preceding paragraphs as though fully set forth herein.

150. CHPayer and CHTech owe BCBSAZ a duty of good faith and fair dealing in

1 connection with the DRG Agreement.

2 151. CHPayer and CHTech violated the implied covenant of good faith and fair dealing
3 when CHP and CHTech reneged on their promises to provide the DRG Services, implement
4 reasonable measures to safeguard BCBSAZ's Confidential Information, and maintain
5 BCBSAZ's access to its Confidential Information and its use of its HRP claims system.

6 152. CHP and CHTech's actions and inactions have prevented BCBSAZ from
7 obtaining the full benefit of the DRG Agreement.

8 153. As a result of this breach, BCBSAZ has suffered damages in an amount to be
9 proven at trial.

10 154. BCBSAZ is also entitled to its costs, expenses and fees, including, without
11 limitation, attorneys' fees and costs incurred in enforcing and collecting the obligations
12 described in this Complaint, pursuant to A.R.S. §§ 12-341 and 12-341.01, and any applicable
13 contractual provisions.

14 **COUNT V**
15 **BREACH OF THE HCA AGREEMENT**
16 **(Against CHSolutions)**

17 155. Plaintiffs incorporate by reference each and every allegation contained in the
18 preceding paragraphs as though fully set forth herein.

19 156. The HCA Agreement is a valid and enforceable agreement between BCBSAZ
20 and CHSolutions.

21 157. CHSolutions has breached its obligations under the HCA Agreement by, among
22 other things, (i) failing and refusing to provide the HCA Services and (ii) allowing
23 unauthorized access to and use of HCA's Confidential Information, as set forth above.

24 158. HCA has been damaged by CHSolution's breaches of its obligations under the
25 HCA Agreement in an amount to be proven at trial.

26 159. HCA is also entitled to its costs, expenses and fees, including, without limitation,
attorneys' fees and costs incurred in enforcing and collecting the obligations described in this

1 Complaint, pursuant to A.R.S. §§ 12-341 and 12-341.01, and any applicable contractual
2 provisions.

3 **COUNT VI**
4 **BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING IN**
5 **CONNECTION WITH HCA AGREEMENT**
6 **(Against CHSolution)**

7 160. Plaintiffs incorporate by reference each and every allegation contained in the
8 preceding paragraphs as though fully set forth herein.

9 161. CHSolution owes BCBSAZ a duty of good faith and fair dealing in connection
10 with the HCA Agreement.

11 162. CHSolution violated the implied covenant of good faith and fair dealing when
12 CHSolution reneged on its promises to provide the HCA Services, implement reasonable
13 measures to safeguard BCBSAZ's Confidential Information, and maintain BCBSAZ's access
14 to its Confidential Information and its use of its HRP claims system.

15 163. CHSolution's actions and inactions have prevented BCBSAZ from obtaining the
16 full benefit of the HCA Agreement.

17 164. As a result of this breach, BCBSAZ has suffered damages in an amount to be
18 proven at trial.

19 165. BCBSAZ is also entitled to its costs, expenses and fees, including, without
20 limitation, attorneys' fees and costs incurred in enforcing and collecting the obligations
21 described in this Complaint, pursuant to A.R.S. §§ 12-341 and 12-341.01, and any applicable
22 contractual provisions.

23 **COUNT VI**
24 **VIOLATION OF THE ARIZONA CONSUMER FRAUD ACT**
25 **(Against all Defendants)**

26 166. Plaintiffs repeat and reallege each and every allegation contained above as if
fully set forth herein.

1 167. This claim is brought by Plaintiffs against Defendants for violation of the
2 Arizona Consumer Fraud Act (“ACFA”), Ariz. Rev. Stat. Ann. § 44-1522 *et seq.*

3 168. The ACFA prohibits deceptive practices, including false promises, “by any
4 person . . . in connection with the sale or advertisement of any merchandise.” *See* A.R.S. § 44-
5 1522(A).

6 169. BCBSAZ is a “person” as defined by the ACFA.

7 170. BCBSAZ was the target of a sale or advertisement of health care services or data
8 security services by CHC. BCBSAZ’s purchase of such services from CHC constitutes a “sale”
9 of “merchandise” under the ACFA. *See* A.R.S. § 44-1521(5)-(7).

10 171. As set forth in more detail above, CHC made various false promises or
11 misrepresentations to BCBSAZ regarding the security measures it had or would implement to
12 safeguard the security of BCBSAZ’s Confidential Information. Those false promises or
13 misrepresentation, including omissions, were contained in the Agreements (including the
14 BAA, the Disaster Recovery Plan, the Delegation Addendum) and it other documents provided
15 to BCBSAZ (including the Information Security Program Overview and CHC’s responses to
16 BCBSAZ’s Company Questionnaire).

17 172. CHC knew or should have known that it utilized outdated and insecure systems
18 to protect its customers’ confidential data.

19 173. CHC knew or should have known that some of its systems had not implemented
20 MFA.

21 174. CHC knew or should have known that its ability to maintain and secure backup
22 copies of Confidential Information was compromised by its outdated system and lack of robust
23 security measures.

24 175. CHC was aware that it did not have the resources, bandwidth or expertise to fulfil
25 the representations regarding its administrative, physical, and technical security safeguards and
26

1 procedures CHC made in the BPaaS Agreement, exhibits thereto, and other external-facing
2 communications to BCBSAZ.

3 176. CHC made these misrepresentations and false promises to BCBSAZ anyway,
4 and thereby omitted providing BCBSAZ with material information regarding the true nature
5 of CHC's ability to secure BCBSAZ's Confidential Information and maintain continued access
6 to BCBSAZ's HRP system.

7 177. CHC's misrepresentations were willful and done with malice.

8 178. BCBSAZ was not aware of these omissions until after the Cyber Event occurred
9 and it was damaged.

10 179. Had CHC disclosed this information to BCBSAZ, BCBSAZ would not have
11 entered into the Agreements with CHC and/or would have terminated those Agreements in
12 favor of alternative vendors capable of providing the requisite security measures.

13 180. Because CHC violated the ACFA, CHC is liable to BCBSAZ for direct and
14 consequential damages, treble damages for willful misconduct, as well as punitive damages.

15 181. BCBSAZ has suffered direct, consequential and proximate damages in reliance
16 on CHC's misrepresentations regarding the extent of its security measures and protocols in
17 amount to be proven at trial.

18 **PRAYER FOR RELIEF**

19 WHEREFORE, Plaintiffs demand Judgment against Defendants, and each of them,
20 jointly and severally, as follows:

- 21 A. For damages to the fullest extent permitted by law, including punitive damages;
- 22 B. For trebling of Plaintiffs' damages pursuant to the ACFA;
- 23 C. For interest at the highest rate allowed by law from the earliest time permitted
24 by law until the judgment is paid in full;
- 25 D. For attorneys' fees and taxable costs pursuant to the Agreements and applicable
26 law including A.R.S. §§ 12-341 and 12-341.01; and

1 E. For such other and further relief as the Court deems just and appropriate under
2 the circumstances.

3 **JURY DEMAND**

4 Plaintiffs demand a trial by jury on all issues so triable in this action.

5 DATED this 13th day of January, 2025.

6 **COPPERSMITH BROCKELMAN PLC**

7
8 By: /s/ Keith Beauchamp

9 Keith Beauchamp

10 Marvin C. Ruth

11 Malvika A. Sinha

12 Kelleen Mull

13 2800 North Central Avenue, Suite 1900

14 Phoenix, Arizona 85004

15 *Attorneys for Plaintiffs*

Person/Attorney Filing: Keith Beauchamp
Mailing Address: 2800 North Central Avenue, Suite 1900
City, State, Zip Code: Phoenix, AZ 85004
Phone Number: (602)381-5490
E-Mail Address: kbeauchamp@cblawyers.com
[☐] Representing Self, Without an Attorney
(If Attorney) State Bar Number: 012434, Issuing State: AZ

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF MARICOPA

BLUE CROSS AND BLUE SHIELD OF
ARIZONA, INC, et al.

Plaintiff(s),

Case No. **CV2025-001530**

v.

CHANGE HEALTHCARE PRACTICE
MANAGEMENT SOLUTIONS, INC., et al.
Defendant(s).

**CERTIFICATE OF
COMPULSORY ARBITRATION**

I certify that I am aware of the dollar limits and any other limitations set forth by the Local Rules of Practice for the Maricopa County Superior Court, and I further certify that this case IS NOT subject to compulsory arbitration, as provided by Rules 72 through 77 of the Arizona Rules of Civil Procedure.

RESPECTFULLY SUBMITTED this January 13, 2025

By: Keith Beauchamp /s/
Plaintiff/Attorney for Plaintiff

EXHIBIT 2

1 Keith Beauchamp (012434)
Marvin C. Ruth (024220)
2 Malvika A. Sinha (038046)
Kelleen Mull (036517)
3 **COPPERSMITH BROCKELMAN PLC**
2800 North Central Avenue, Suite 1900
4 Phoenix, Arizona 85004
T: (602) 381-5490
5 F: (602) 224-6020
kbeauchamp@cblawyers.com
6 mruth@cblawyers.com
msinha@cblawyers.com
7 kmull@cblawyers.com

8 *Attorneys for Plaintiffs*

9
10 **SUPERIOR COURT OF ARIZONA**

11 **COUNTY OF MARICOPA**

12 BLUE CROSS AND BLUE SHIELD OF
ARIZONA, INC., an Arizona non-profit
13 corporation; and HEALTH CHOICE
ARIZONA, INC., an Arizona corporation,

14 Plaintiffs,

15 v.

16 CHANGE HEALTHCARE PRACTICE
MANAGEMENT SOLUTIONS, INC., a
17 Delaware corporation; CHANGE
HEALTHCARE TECHNOLOGIES, LLC,
18 a Delaware limited liability company;
CHANGE HEALTHCARE SOLUTIONS,
19 LLC, a Delaware limited liability company;
20 and CHANGE HEALTHCARE PAYER
PAYMENT INTEGRITY, LLC, a
21 Delaware limited liability company,

22 Defendants.

No. CV2025-001530

ACCEPTANCE OF SERVICE

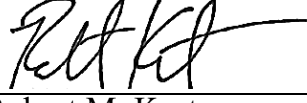
(Assigned to the Hon. Christopher Whitten)

23 I, Robert M. Kort, as attorney for Defendants Change Healthcare Practice Management
24 Solutions, Inc., Change Healthcare Technologies, LLC, Change Healthcare Solutions, LLC
25 and Change Healthcare Payer Payment Integrity, LLC ("Defendants"), acknowledge receipt of
26 true and correct copies of the Summons, Complaint and Certificate on Compulsory Arbitration

1 in this matter, and accept service of those documents as if they had been personally served
2 upon Defendants. By this acceptance of service, Defendants do not waive any defenses to the
3 claims made by Plaintiffs in this matter. Defendants shall have 45 days from the date of
4 acceptance to file a response to the Complaint.

5 DATED this 12th day of February, 2025.

6 **WOMBLE BOND DICKINSON (US) LLP**

7 By: 
8 Robert M. Kort
9 201 East Washington Street, Suite 1200
10 Phoenix, AZ 85004
Counsel for Defendants

11 **ORIGINAL E-FILED** February 13, 2025 to:

12
13 /s/ Verna Colwell
14
15
16
17
18
19
20
21
22
23
24
25
26